5

rney Docket No.: CIG-103

ABSTRACT OF THE DISCLOSURE

An intrusion detection system (IDS) that uses application monitors for detecting application-based attacks against computer systems. The IDS implements application monitors in the form of a software program to learn and monitor the behavior of system programs in order to detect attacks against computer hosts. The application monitors implement machine learning algorithms to provide a mechanism for learning from previously observed behavior in order to recognize future attacks that it has not seen before. The application monitors include temporal locality algorithms to increased the accuracy of the IDS. The IDS of the present invention may comprise a string-matching program, a neural network, or a time series prediction algorithm for learning normal application behavior and for detecting anomalies.

Document #: 1027467 v.3

Document #: 1027467 v.3